

1
2
3
4
5
IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE
6
7

8 LEO GUY, individually and on behalf all
9 others similarly situated,
10

Plaintiffs,

v.

11 CONVERGENT OUTSOURCING, INC.,
12

Defendant.

No.

CLASS ACTION COMPLAINT

JURY DEMAND

13
14 **CLASS ACTION COMPLAINT**

15 Plaintiff(s) Leo Guy (“Plaintiff(s)”) bring this action, on behalf of themselves and all
16 others similarly situated, against Defendant Convergent Outsourcing, Inc. (“Convergent” or
17 “Defendant”). Plaintiff(s) seek to obtain damages, restitution, and injunctive relief for a class of
18 individuals (“Class” or “Class Members”) who are similarly situated and have received notices
19 of the data breach from Convergent. Plaintiff(s) make the following allegations upon information
20 and belief, except as to their own actions, the investigation of their counsel, and the facts that are
a matter of public record.

21
22 **I. NATURE OF THE ACTION**

23 1. This class action arises out of a 2022 data breach (“Data Breach”) of documents
24 and information stored on the computer network of Convergent, a third-party debt collection
company that serves the telecommunication, utility, banking, cable company, and financial

1 service industries by offering consumer debt collection.¹

2. According to its website, “Convergent believe[s] in customer service”² and claims
 3 “[they] want to make it easy as possible for people to pay the debts they owe.”³

3. On its computer network, Convergent holds and stores certain highly sensitive
 4 personally identifiable information (“PII” or “Private Information”) of the Plaintiff(s) and the
 5 putative Class Members, who are customers of companies that Convergent provides debt
 6 collection services for, i.e., individuals who provided their highly sensitive and private
 7 information in exchange for business services.

4. According to the Notice of Data Breach Letter that Convergent sent to Plaintiff(s)
 5 and Class members, it first became aware of the Data Breach on June 17, 2022, and began
 6 investigating.⁴

5. Convergent finally began notifying the unknown or undisclosed number of
 6 victims over 4 months after the “data breach” occurred, stating that their PII had been stolen in
 7 what Defendant calls an “interruption to certain services performed by Convergent affecting
 8 certain computer systems.”⁵

6. Convergent also admits that “an external actor gained unauthorized access to our
 7 systems and deployed a ransomware malware” and that its “investigation also revealed that the
 8 unauthorized actor deployed certain data extraction tools on one storage drive that is used to save
 9 and share files internally.”⁶

7. As a result of Convergent’s Data Breach, Plaintiff(s) and thousands (if not more)
 8 of Class Members suffered ascertainable losses in the form of the loss of the benefit of their
 9 bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or
 10

21 ¹ <https://www.convergentusa.com/outsourcing/question/list?type=A> (last accessed November 1, 2022)

22 ² <https://www.convergentusa.com/outsourcing/site/who-is-convergent-outsourcing> (last accessed on
 November 1, 2022).

23 ³ *Id.*

24 ⁴ See Exhibit A, Plaintiff(s)’ Notice Letter.

⁵ *Id.*

⁶ *Id.*

1 mitigate the effects of the attack.

2 8. In addition, Plaintiff(s)' and Class Members' sensitive personal information—
 3 which was entrusted to Defendant—who claims in the Data Breach Letter that “[they] take the
 4 confidentiality, privacy, and security of information in our care seriously”⁷—was compromised
 and unlawfully accessed and extracted during the Data Breach.

5 9. Based upon Convergent's notice letter, the Private Information compromised in
 6 the Data Breach was intentionally accessed and removed, also called exfiltrated, by the cyber-
 7 criminals who perpetrated this attack and remains in the hands of those cyber-criminals.

8 10. The Data Breach was a direct result of Defendant's failure to implement adequate
 9 and reasonable cyber-security procedures and protocols necessary to protect Plaintiff(s) and
 10 Class Members' Private Information.

11 11. Plaintiff(s) bring this class action lawsuit on behalf of those similarly situated to
 12 address Defendant's inadequate safeguarding of Class Members' Private Information that they
 13 collected and maintained, and for failing to provide timely and adequate notice to Plaintiff(s) and
 14 other Class Members that their information had been subject to the unauthorized access of an
 15 unknown third party and precisely what specific type of information was accessed.

16 12. Defendant maintained the Private Information in a reckless manner. In particular,
 17 the Private Information was maintained on Defendant's computer network in a condition
 18 vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper
 19 disclosure of Plaintiff(s)' and Class Members' Private Information was a known risk to
 20 Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the
 21 Private Information from those risks left that property in a dangerous condition.

22 13. Defendant disregarded the privacy and property rights of Plaintiff(s) and Class
 23 Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate
 24 and reasonable measures to ensure its data systems were protected against unauthorized

⁷ *Id.*

1 intrusions; failing to disclose that they did not have adequately robust computer systems and
2 security practices to safeguard Class Members' Private Information; failing to take standard and
3 reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and
4 Class Members prompt and accurate and complete notice of the Data Breach.

5 14. In addition, Defendant and its employees failed to properly monitor the computer
6 network and systems that housed the Private Information. Had Defendant properly monitored its
7 computers, it would have discovered the intrusion sooner, and potentially been able to mitigate
8 the injuries to Plaintiff(s) and the Class.

9 15. Plaintiff(s)' and Class Members' identities are now at substantial and imminent
10 risk because of Defendant's negligent conduct since the Private Information that Defendant
11 collected and maintained (including Social Security numbers) is now in the hands of data thieves.

12 16. Armed with the Private Information accessed in the Data Breach, data thieves can
13 commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members'
14 names, taking out loans in Class Members' names, using Class Members' information to obtain
15 government benefits, filing fraudulent tax returns using Class Members' information, filing false
16 medical claims using Class Members' information, obtaining driver's licenses in Class Members'
17 names but with another person's photograph, and giving false information to police during an
18 arrest.

19 17. As a result of the Data Breach, Plaintiff(s) and Class Members have been exposed
20 to a heightened and imminent risk of fraud and identity theft. Plaintiff(s) and Class Members
21 must now and in the future closely monitor their financial accounts to guard against identity theft.

22 18. Plaintiff(s) and Class Members may also incur out of pocket costs for, *e.g.*,
23 purchasing credit monitoring services, credit freezes, credit reports, or other protective measures
24 to deter and detect identity theft.

25 19. Through this Complaint, Plaintiff(s) seek to remedy these harms on behalf of
26 themselves and all similarly situated individuals whose Private Information was accessed during
27 the Data Breach (the "Class").

20. Accordingly, Plaintiff(s) bring this action against Defendant for negligence, negligence per se, breach of implied contract, unjust enrichment, and declaratory relief, seeking redress for Convergent's unlawful conduct.

21. Plaintiff(s) seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

II. PARTIES

22. Plaintiff Leo Guy is, and at all times relevant to this Complaint was, an individual citizen of the State of New Hampshire, residing in the city of Derry (Rockingham County). On or about October 31, 2022, Plaintiff Guy received a Notice of the Data Breach from Convergent Outsourcing, Inc. A copy of the notice they received is dated October 26, 2022, and attached as Exhibit A (the “Notice Letter”).

23. Defendant Convergent Outsourcing, Inc., is a Washington for-profit corporation. Convergent's principal place of business is located at 800 SW 39th Street, Suite 100, Renton, Washington 98057. Defendant can be served through its registered agent at: CT Corporation System, 711 Capitol Way South, Suite 204, Olympia, Washington 98501.

24. According to its notice letter, the business operations of Convergent's affiliate, Account Control Technology, Inc. ("ACT") were also affected by the same Data Breach.⁸ Upon information and belief, both Convergent and ACT are subsidiaries of Account Control Technology Holdings, Inc.⁹

25. All of Plaintiff(s)' claims stated herein are asserted against Defendant Convergent, and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action under 28 U.S.C.

8 *Id.*

⁹ <https://accountcontrol.com/About-Us/History> (last accessed November 1, 2022).

1 § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or
 2 value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the
 3 proposed class, and at least one member of the class is a citizen of a state different from
 4 Defendant.

5 27. The Court has general personal jurisdiction over Defendant because, personally
 6 or through its agents, Defendant operates, conducts, engages in, or carries on a business or
 7 business venture in Washington; it is registered with the Secretary of State in Washington as a
 8 for-profit corporation; it maintains its headquarters in Washington; and committed tortious acts
 9 in Washington.

10 28. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the
 11 district within which Convergent has the most significant contacts.

12 IV. STATEMENT OF FACTS

13 **Nature of Defendant's Business.**

14 29. Convergent started its business as a debt collection agency in 1950. Convergent
 15 has approximately 1,000 employees globally in the United States, Asia, Europe, and Africa while
 16 maintaining its headquarters in Renton, Washington.¹⁰

17 30. Prior to collecting consumer debt, Convergent collects PII of consumers from
 18 companies seeking Convergent's debt collection services. This PII includes, *inter alia*,
 19 consumers' names, contact information, Social Security numbers, and financial account
 20 information.

21 31. Convergent, in the regular course of its business, collects and maintains the PII of
 22 consumers (on behalf of its customers) as a requirement of its business practices.

23 32. Consumers entrusted the customers of Convergent with their PII with the mutual
 24 understanding that this highly sensitive private information was confidential and would be
 25 properly safeguarded from misuse and theft.

26
 27
 28
 29
 30
 31
 32
 33
 34
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45
 46
 47
 48
 49
 50
 51
 52
 53
 54
 55
 56
 57
 58
 59
 60
 61
 62
 63
 64
 65
 66
 67
 68
 69
 70
 71
 72
 73
 74
 75
 76
 77
 78
 79
 80
 81
 82
 83
 84
 85
 86
 87
 88
 89
 90
 91
 92
 93
 94
 95
 96
 97
 98
 99
 100
 101
 102
 103
 104
 105
 106
 107
 108
 109
 110
 111
 112
 113
 114
 115
 116
 117
 118
 119
 120
 121
 122
 123
 124
 125
 126
 127
 128
 129
 130
 131
 132
 133
 134
 135
 136
 137
 138
 139
 140
 141
 142
 143
 144
 145
 146
 147
 148
 149
 150
 151
 152
 153
 154
 155
 156
 157
 158
 159
 160
 161
 162
 163
 164
 165
 166
 167
 168
 169
 170
 171
 172
 173
 174
 175
 176
 177
 178
 179
 180
 181
 182
 183
 184
 185
 186
 187
 188
 189
 190
 191
 192
 193
 194
 195
 196
 197
 198
 199
 200
 201
 202
 203
 204
 205
 206
 207
 208
 209
 210
 211
 212
 213
 214
 215
 216
 217
 218
 219
 220
 221
 222
 223
 224
 225
 226
 227
 228
 229
 230
 231
 232
 233
 234
 235
 236
 237
 238
 239
 240
 241
 242
 243
 244
 245
 246
 247
 248
 249
 250
 251
 252
 253
 254
 255
 256
 257
 258
 259
 260
 261
 262
 263
 264
 265
 266
 267
 268
 269
 270
 271
 272
 273
 274
 275
 276
 277
 278
 279
 280
 281
 282
 283
 284
 285
 286
 287
 288
 289
 290
 291
 292
 293
 294
 295
 296
 297
 298
 299
 300
 301
 302
 303
 304
 305
 306
 307
 308
 309
 310
 311
 312
 313
 314
 315
 316
 317
 318
 319
 320
 321
 322
 323
 324
 325
 326
 327
 328
 329
 330
 331
 332
 333
 334
 335
 336
 337
 338
 339
 340
 341
 342
 343
 344
 345
 346
 347
 348
 349
 350
 351
 352
 353
 354
 355
 356
 357
 358
 359
 360
 361
 362
 363
 364
 365
 366
 367
 368
 369
 370
 371
 372
 373
 374
 375
 376
 377
 378
 379
 380
 381
 382
 383
 384
 385
 386
 387
 388
 389
 390
 391
 392
 393
 394
 395
 396
 397
 398
 399
 400
 401
 402
 403
 404
 405
 406
 407
 408
 409
 410
 411
 412
 413
 414
 415
 416
 417
 418
 419
 420
 421
 422
 423
 424
 425
 426
 427
 428
 429
 430
 431
 432
 433
 434
 435
 436
 437
 438
 439
 440
 441
 442
 443
 444
 445
 446
 447
 448
 449
 450
 451
 452
 453
 454
 455
 456
 457
 458
 459
 460
 461
 462
 463
 464
 465
 466
 467
 468
 469
 470
 471
 472
 473
 474
 475
 476
 477
 478
 479
 480
 481
 482
 483
 484
 485
 486
 487
 488
 489
 490
 491
 492
 493
 494
 495
 496
 497
 498
 499
 500
 501
 502
 503
 504
 505
 506
 507
 508
 509
 510
 511
 512
 513
 514
 515
 516
 517
 518
 519
 520
 521
 522
 523
 524
 525
 526
 527
 528
 529
 530
 531
 532
 533
 534
 535
 536
 537
 538
 539
 540
 541
 542
 543
 544
 545
 546
 547
 548
 549
 550
 551
 552
 553
 554
 555
 556
 557
 558
 559
 560
 561
 562
 563
 564
 565
 566
 567
 568
 569
 570
 571
 572
 573
 574
 575
 576
 577
 578
 579
 580
 581
 582
 583
 584
 585
 586
 587
 588
 589
 590
 591
 592
 593
 594
 595
 596
 597
 598
 599
 600
 601
 602
 603
 604
 605
 606
 607
 608
 609
 610
 611
 612
 613
 614
 615
 616
 617
 618
 619
 620
 621
 622
 623
 624
 625
 626
 627
 628
 629
 630
 631
 632
 633
 634
 635
 636
 637
 638
 639
 640
 641
 642
 643
 644
 645
 646
 647
 648
 649
 650
 651
 652
 653
 654
 655
 656
 657
 658
 659
 660
 661
 662
 663
 664
 665
 666
 667
 668
 669
 670
 671
 672
 673
 674
 675
 676
 677
 678
 679
 680
 681
 682
 683
 684
 685
 686
 687
 688
 689
 690
 691
 692
 693
 694
 695
 696
 697
 698
 699
 700
 701
 702
 703
 704
 705
 706
 707
 708
 709
 710
 711
 712
 713
 714
 715
 716
 717
 718
 719
 720
 721
 722
 723
 724
 725
 726
 727
 728
 729
 730
 731
 732
 733
 734
 735
 736
 737
 738
 739
 740
 741
 742
 743
 744
 745
 746
 747
 748
 749
 750
 751
 752
 753
 754
 755
 756
 757
 758
 759
 760
 761
 762
 763
 764
 765
 766
 767
 768
 769
 770
 771
 772
 773
 774
 775
 776
 777
 778
 779
 780
 781
 782
 783
 784
 785
 786
 787
 788
 789
 790
 791
 792
 793
 794
 795
 796
 797
 798
 799
 800
 801
 802
 803
 804
 805
 806
 807
 808
 809
 810
 811
 812
 813
 814
 815
 816
 817
 818
 819
 820
 821
 822
 823
 824
 825
 826
 827
 828
 829
 830
 831
 832
 833
 834
 835
 836
 837
 838
 839
 840
 841
 842
 843
 844
 845
 846
 847
 848
 849
 850
 851
 852
 853
 854
 855
 856
 857
 858
 859
 860
 861
 862
 863
 864
 865
 866
 867
 868
 869
 870
 871
 872
 873
 874
 875
 876
 877
 878
 879
 880
 881
 882
 883
 884
 885
 886
 887
 888
 889
 890
 891
 892
 893
 894
 895
 896
 897
 898
 899
 900
 901
 902
 903
 904
 905
 906
 907
 908
 909
 910
 911
 912
 913
 914
 915
 916
 917
 918
 919
 920
 921
 922
 923
 924
 925
 926
 927
 928
 929
 930
 931
 932
 933
 934
 935
 936
 937
 938
 939
 940
 941
 942
 943
 944
 945
 946
 947
 948
 949
 950
 951
 952
 953
 954
 955
 956
 957
 958
 959
 960
 961
 962
 963
 964
 965
 966
 967
 968
 969
 970
 971
 972
 973
 974
 975
 976
 977
 978
 979
 980
 981
 982
 983
 984
 985
 986
 987
 988
 989
 990
 991
 992
 993
 994
 995
 996
 997
 998
 999
 1000
 1001
 1002
 1003
 1004
 1005
 1006
 1007
 1008
 1009
 1010
 1011
 1012
 1013
 1014
 1015
 1016
 1017
 1018
 1019
 1020
 1021
 1022
 1023
 1024
 1025
 1026
 1027
 1028
 1029
 1030
 1031
 1032
 1033
 1034
 1035
 1036
 1037
 1038
 1039
 1040
 1041
 1042
 1043
 1044
 1045
 1046
 1047
 1048
 1049
 1050
 1051
 1052
 1053
 1054
 1055
 1056
 1057
 1058
 1059
 1060
 1061
 1062
 1063
 1064
 1065
 1066
 1067
 1068
 1069
 1070
 1071
 1072
 1073
 1074
 1075
 1076
 1077
 1078
 1079
 1080
 1081
 1082
 1083
 1084
 1085
 1086
 1087
 1088
 1089
 1090
 1091
 1092
 1093
 1094
 1095
 1096
 1097
 1098
 1099
 1100
 1101
 1102
 1103
 1104
 1105
 1106
 1107
 1108
 1109
 1110
 1111
 1112
 1113
 1114
 1115
 1116
 1117
 1118
 1119
 1120
 1121
 1122
 1123
 1124
 1125
 1126
 1127
 1128
 1129
 1130
 1131
 1132
 1133
 1134
 1135
 1136
 1137
 1138
 1139
 1140
 1141
 1142
 1143
 1144
 1145
 1146
 1147
 1148
 1149
 1150
 1151
 1152
 1153
 1154
 1155
 1156
 1157
 1158
 1159
 1160
 1161
 1162
 1163
 1164
 1165
 1166
 1167
 1168
 1169
 1170
 1171
 1172
 1173
 1174
 1175
 1176
 1177
 1178
 1179
 1180
 1181
 1182
 1183
 1184
 1185
 1186
 1187
 1188
 1189
 1190
 1191
 1192
 1193
 1194
 1195
 1196
 1197
 1198
 1199
 1200
 1201
 1202
 1203
 1204
 1205
 1206
 1207
 1208
 1209
 1210
 1211
 1212
 1213
 1214
 1215
 1216
 1217
 1218
 1219
 1220
 1221
 1222
 1223
 1224
 1225
 1226
 1227
 1228
 1229
 1230
 1231
 1232
 1233
 1234
 1235
 1236
 1237
 1238
 1239
 1240
 1241
 1242
 1243
 1244
 1245
 1246
 1247
 1248
 1249
 1250
 1251
 1252
 1253
 1254
 1255
 1256
 1257
 1258
 1259
 1260
 1261
 1262
 1263
 1264
 1265
 1266
 1267
 1268
 1269
 1270
 1271
 1272
 1273
 1274
 1275
 1276
 1277
 1278
 1279
 1280
 1281
 1282
 1283
 1284
 1285
 1286
 1287
 1288
 1289
 1290
 1291
 1292
 1293
 1294
 1295
 1296
 1297
 1298
 1299
 1300
 1301
 1302
 1303
 1304
 1305
 1306
 1307
 1308
 1309
 1310
 1311
 1312
 1313
 1314
 1315
 1316
 1317
 1318
 1319
 1320
 1321
 1322
 1323
 1324
 1325
 1326
 1327
 1328
 1329
 1330
 1331
 1332
 1333
 1334
 1335
 1336
 1337
 1338
 1339
 1340
 1341
 1342
 1343
 1344
 1345
 1346
 1347
 1348
 1349
 1350
 1351
 1352
 1353
 1354
 1355
 1356
 1357
 1358
 1359
 1360
 1361
 1362
 1363
 1364
 1365
 1366
 1367
 1368
 1369
 1370
 1371
 1372
 1373
 1374
 1375
 1376
 1377
 1378
 1379
 1380
 1381
 1382
 1383
 1384
 1385
 1386
 1387
 1388
 1389
 1390
 1391
 1392
 1393
 1394
 1395
 1396
 1397
 1398
 1399
 1400
 1401
 1402
 1403
 1404
 1405
 1406
 1407
 1408
 1409
 1410
 1411
 1412
 1413
 1414
 1415
 1416
 1417
 1418
 1419
 1420
 1421
 1422
 1423
 1424
 1425
 1426
 1427
 1428
 1429
 1430
 1431
 1432
 1433
 1434
 1435
 1436
 1437
 1438
 1439
 1440
 1441
 1442
 1443
 1444
 1445
 1446
 1447
 1448
 1449
 1450
 1451
 1452
 1453

1 33. Convergent promises in its Privacy Policy that they “incorporate commercially
 2 reasonable safeguards to help protect and secure your Personal Information.”¹¹

3 34. In its California Online Privacy Policy, Convergent acknowledges that it is
 4 susceptible to data breaches and ransomware threats, acknowledging it must “detect security
 5 incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting
 6 those responsible for that activity.”¹² Moreover, Convergent is aware that it must: comply with
 7 federal, state, and local laws; protect the safety, rights, property or security of consumers and
 8 third parties; and detect, prevent, or otherwise address fraud, security, or technical issues.¹³

9 35. In the course of collecting Private Information from consumers, including
 10 Plaintiff(s) and Class Members, Convergent promised to provide confidentiality and adequate
 11 security for Private Information through its applicable Privacy Policy and in compliance with
 12 statutory privacy requirements applicable to the servicing industry.

13 36. In its Notice Letters to Plaintiff(s) and Class Members, Convergent claims that
 14 “the confidentiality, privacy, and security of information in our care are among our highest
 15 priorities.”¹⁴

16 37. Plaintiff(s) and the Class Members, as consumers, relied on the promises and
 17 duties of Convergent to keep their sensitive PII confidential and securely maintained, to use this
 18 information for business purposes only, and to make only authorized disclosures of this
 19 information. Consumers, in general, demand that businesses that require highly sensitive PII will
 20 provide security to safeguard their PII, especially when Social Security numbers are involved.

21 38. In the course of their dealings, Plaintiff(s) and Class Members provided
 22 Convergent (either directly or through Convergent’s business customers) with all or most of the
 23 following types of Private Information:

24 ¹¹ <https://www.convergentusa.com/outsourcing/page/privacy-policy> (last accessed on November 1, 2022).

25 ¹² <https://www.convergentusa.com/outsourcing/page/ccpa-policy> (last accessed on November 1, 2022).

26 ¹³ *Id.*

27 ¹⁴ See Notice Letter, Ex. A.

- 1 • First and last names;
- 2 • Home addresses;
- 3 • Email addresses;
- 4 • Phone numbers;
- 5 • Social Security numbers;
- 6 • Employers;
- 7 • Account numbers; and
- 8 • Bank account or payment card information.¹⁵

9 39. Convergent had a duty to adopt reasonable measures to protect Plaintiff(s)' and
 10 Class Members' PII from unauthorized disclosure to third parties.

11 **The Data Breach.**

12 40. According to its Notice Letters, on June 17, 2022, Convergent "became aware of
 13 an interruption to certain services." After an unspecified amount of time, between the date they
 14 "became aware" and sent the notice letters, its investigation determined that an "unauthorized
 15 actor" accessed the Convergent network and "deployed certain extraction tools on one storage
 16 drive that is used to save and share files internally."¹⁶

17 41. The letter does not identify how long before detection the "interruption" was
 18 occurring.¹⁷

19 42. By October 26, 2022, according to Convergent's own Notice Letters, it was aware
 20 that the Data Breach included "name[s], contact information, financial account number[s], Social
 21 Security number[s],"¹⁸ including that of Plaintiff(s). Convergent does not why the Notice Letters
 22 were not sent until over 4 months later, time which could have helped Plaintiff(s) and Class
 23 members mitigate the damages suffered from Convergent's Data Breach.

24 ¹⁵ See *id.*; see also <https://www.convergentusa.com/outsourcing/page/privacy-policy> (last accessed on
 25 November 1, 2022).

26 ¹⁶ Notice Letter, Ex. A.

27 ¹⁷ *Id.*

28 ¹⁸ *Id.*

1 43. A review of various State Attorneys General websites shows that, to-date,
 2 Convergent has not yet notified the State Attorney Generals of this Data Breach, as required by
 3 the laws of the states.¹⁹ Convergent did not notify government agencies or the public about the
 4 Data Breach except through the Notice letters received by Plaintiff(s) and Class members over 4
 months after the breach was discovered.

5 44. Moreover, Convergent has failed to expeditiously report how many individuals'
 6 records were exfiltrated during its Data Breach, as required by various state's laws.²⁰

7 45. Therefore, ***Plaintiff(s)'s and Class members' PII was in the hands of***
 8 ***cybercriminals for over 4 months before they were notified*** of Convergent's Data Breach. Time
 9 is of the essence when trying to protect against identity theft after a data breach, so early
 10 notification is critical.

11 46. Because of this targeted, intentional cyberattack, data thieves were able to gain
 12 access to and obtain data from Convergent that included the Private Information of Plaintiff(s)
 13 and Class Members.

14 47. Convergent admits that the files exfiltrated from Convergent contained at least the
 15 following information of Plaintiff(s) and Class Members: names, contact information, financial
 16 account numbers, and Social Security numbers.

17 48. Upon information and belief, the Private Information stored on Convergent's
 18 network was not encrypted.

19 49. Plaintiff(s)' Private Information was accessed and stolen in the Data Breach.
 20 Plaintiff(s) reasonably believe their stolen Private Information is currently available for sale on

21 ¹⁹ See, e.g., Maine: <https://apps.web.main.gov/online/aeviwer/ME/40/list.shtml> showing "No entries
 22 found"; Texas: <https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage>
 23 showing "No matching records found"; California:
https://oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=convergent&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D=
 24 "There are currently no published reported breaches" (last accessed on November 1, 2022).

²⁰ See, e.g., Maine's requirements at https://www.maine.gov/ag/consumer/identity_theft/index.shtml
 (last accessed on November 1, 2022).

1 the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that
 2 collect highly sensitive Private Information.

3 50. As a result of the Data Breach, Convergent now encourages Class Members to
 4 enroll in credit monitoring, fraud consultation, and identity theft restoration services, a tacit
 5 admission of the imminent risk of identity theft faced by Plaintiff(s) and Class members.²¹

6 51. That Convergent is encouraging Plaintiff(s) and Class Members to enroll in credit
 7 monitoring and identity theft restoration services is an acknowledgment that the impacted
 8 consumers are subject to a substantial and imminent threat of fraud and identity theft.

9 52. Convergent had obligations created by contract, industry standards, and common
 10 law to keep Plaintiff(s)'s and Class Members' Private Information confidential and to protect it
 11 from unauthorized access and disclosure.

12 53. Convergent could have prevented this Data Breach by, among other things,
 13 properly encrypting or otherwise protecting their equipment and computer files containing PII.

14 ***Defendant Acquires, Collects, and Stores Plaintiff(s)'s and Class Members' PII.***

15 54. Convergent acquires, collects, and stores a massive amount of PII of consumers
 16 for its business purposes as it provides debt collection services to third-party businesses (*i.e.*,
 17 Convergent's customers). Upon information and belief, Convergent may not be properly deleting
 18 or destroying the PII records of its former customers or for those consumers whose debts have
 19 been fully satisfied.

20 55. By obtaining, collecting, and using Plaintiff(s)' and Class Members' PII for its
 21 own financial gain and business purposes, Defendant assumed legal and equitable duties and
 22 knew that it was responsible for protecting Plaintiff(s)' and Class Members' PII from disclosure.

23 56. Plaintiff(s) and the Class Members have taken reasonable steps to maintain the
 24 confidentiality of their PII.

25 57. Plaintiff(s) and the Class Members relied on Defendant to keep their PII

26
 27
 28
 29
 30
 31
 32
 33
 34
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45
 46
 47
 48
 49
 50
 51
 52
 53
 54
 55
 56
 57
 58
 59
 60
 61
 62
 63
 64
 65
 66
 67
 68
 69
 70
 71
 72
 73
 74
 75
 76
 77
 78
 79
 80
 81
 82
 83
 84
 85
 86
 87
 88
 89
 90
 91
 92
 93
 94
 95
 96
 97
 98
 99
 100
 101
 102
 103
 104
 105
 106
 107
 108
 109
 110
 111
 112
 113
 114
 115
 116
 117
 118
 119
 120
 121
 122
 123
 124
 125
 126
 127
 128
 129
 130
 131
 132
 133
 134
 135
 136
 137
 138
 139
 140
 141
 142
 143
 144
 145
 146
 147
 148
 149
 150
 151
 152
 153
 154
 155
 156
 157
 158
 159
 160
 161
 162
 163
 164
 165
 166
 167
 168
 169
 170
 171
 172
 173
 174
 175
 176
 177
 178
 179
 180
 181
 182
 183
 184
 185
 186
 187
 188
 189
 190
 191
 192
 193
 194
 195
 196
 197
 198
 199
 200
 201
 202
 203
 204
 205
 206
 207
 208
 209
 210
 211
 212
 213
 214
 215
 216
 217
 218
 219
 220
 221
 222
 223
 224
 225
 226
 227
 228
 229
 230
 231
 232
 233
 234
 235
 236
 237
 238
 239
 240
 241
 242
 243
 244
 245
 246
 247
 248
 249
 250
 251
 252
 253
 254
 255
 256
 257
 258
 259
 260
 261
 262
 263
 264
 265
 266
 267
 268
 269
 270
 271
 272
 273
 274
 275
 276
 277
 278
 279
 280
 281
 282
 283
 284
 285
 286
 287
 288
 289
 290
 291
 292
 293
 294
 295
 296
 297
 298
 299
 300
 301
 302
 303
 304
 305
 306
 307
 308
 309
 310
 311
 312
 313
 314
 315
 316
 317
 318
 319
 320
 321
 322
 323
 324
 325
 326
 327
 328
 329
 330
 331
 332
 333
 334
 335
 336
 337
 338
 339
 340
 341
 342
 343
 344
 345
 346
 347
 348
 349
 350
 351
 352
 353
 354
 355
 356
 357
 358
 359
 360
 361
 362
 363
 364
 365
 366
 367
 368
 369
 370
 371
 372
 373
 374
 375
 376
 377
 378
 379
 380
 381
 382
 383
 384
 385
 386
 387
 388
 389
 390
 391
 392
 393
 394
 395
 396
 397
 398
 399
 400
 401
 402
 403
 404
 405
 406
 407
 408
 409
 410
 411
 412
 413
 414
 415
 416
 417
 418
 419
 420
 421
 422
 423
 424
 425
 426
 427
 428
 429
 430
 431
 432
 433
 434
 435
 436
 437
 438
 439
 440
 441
 442
 443
 444
 445
 446
 447
 448
 449
 450
 451
 452
 453
 454
 455
 456
 457
 458
 459
 460
 461
 462
 463
 464
 465
 466
 467
 468
 469
 470
 471
 472
 473
 474
 475
 476
 477
 478
 479
 480
 481
 482
 483
 484
 485
 486
 487
 488
 489
 490
 491
 492
 493
 494
 495
 496
 497
 498
 499
 500
 501
 502
 503
 504
 505
 506
 507
 508
 509
 510
 511
 512
 513
 514
 515
 516
 517
 518
 519
 520
 521
 522
 523
 524
 525
 526
 527
 528
 529
 530
 531
 532
 533
 534
 535
 536
 537
 538
 539
 540
 541
 542
 543
 544
 545
 546
 547
 548
 549
 550
 551
 552
 553
 554
 555
 556
 557
 558
 559
 560
 561
 562
 563
 564
 565
 566
 567
 568
 569
 570
 571
 572
 573
 574
 575
 576
 577
 578
 579
 580
 581
 582
 583
 584
 585
 586
 587
 588
 589
 590
 591
 592
 593
 594
 595
 596
 597
 598
 599
 600
 601
 602
 603
 604
 605
 606
 607
 608
 609
 610
 611
 612
 613
 614
 615
 616
 617
 618
 619
 620
 621
 622
 623
 624
 625
 626
 627
 628
 629
 630
 631
 632
 633
 634
 635
 636
 637
 638
 639
 640
 641
 642
 643
 644
 645
 646
 647
 648
 649
 650
 651
 652
 653
 654
 655
 656
 657
 658
 659
 660
 661
 662
 663
 664
 665
 666
 667
 668
 669
 670
 671
 672
 673
 674
 675
 676
 677
 678
 679
 680
 681
 682
 683
 684
 685
 686
 687
 688
 689
 690
 691
 692
 693
 694
 695
 696
 697
 698
 699
 700
 701
 702
 703
 704
 705
 706
 707
 708
 709
 710
 711
 712
 713
 714
 715
 716
 717
 718
 719
 720
 721
 722
 723
 724
 725
 726
 727
 728
 729
 730
 731
 732
 733
 734
 735
 736
 737
 738
 739
 740
 741
 742
 743
 744
 745
 746
 747
 748
 749
 750
 751
 752
 753
 754
 755
 756
 757
 758
 759
 760
 761
 762
 763
 764
 765
 766
 767
 768
 769
 770
 771
 772
 773
 774
 775
 776
 777
 778
 779
 780
 781
 782
 783
 784
 785
 786
 787
 788
 789
 790
 791
 792
 793
 794
 795
 796
 797
 798
 799
 800
 801
 802
 803
 804
 805
 806
 807
 808
 809
 8010
 8011
 8012
 8013
 8014
 8015
 8016
 8017
 8018
 8019
 8020
 8021
 8022
 8023
 8024
 8025
 8026
 8027
 8028
 8029
 8030
 8031
 8032
 8033
 8034
 8035
 8036
 8037
 8038
 8039
 8040
 8041
 8042
 8043
 8044
 8045
 8046
 8047
 8048
 8049
 8050
 8051
 8052
 8053
 8054
 8055
 8056
 8057
 8058
 8059
 8060
 8061
 8062
 8063
 8064
 8065
 8066
 8067
 8068
 8069
 8070
 8071
 8072
 8073
 8074
 8075
 8076
 8077
 8078
 8079
 8080
 8081
 8082
 8083
 8084
 8085
 8086
 8087
 8088
 8089
 8090
 8091
 8092
 8093
 8094
 8095
 8096
 8097
 8098
 8099
 80100
 80101
 80102
 80103
 80104
 80105
 80106
 80107
 80108
 80109
 80110
 80111
 80112
 80113
 80114
 80115
 80116
 80117
 80118
 80119
 80120
 80121
 80122
 80123
 80124
 80125
 80126
 80127
 80128
 80129
 80130
 80131
 80132
 80133
 80134
 80135
 80136
 80137
 80138
 80139
 80140
 80141
 80142
 80143
 80144
 80145
 80146
 80147
 80148
 80149
 80150
 80151
 80152
 80153
 80154
 80155
 80156
 80157
 80158
 80159
 80160
 80161
 80162
 80163
 80164
 80165
 80166
 80167
 80168
 80169
 80170
 80171
 80172
 80173
 80174
 80175
 80176
 80177
 80178
 80179
 80180
 80181
 80182
 80183
 80184
 80185
 80186
 80187
 80188
 80189
 80190
 80191
 80192
 80193
 80194
 80195
 80196
 80197
 80198
 80199
 80200
 80201
 80202
 80203
 80204
 80205
 80206
 80207
 80208
 80209
 80210
 80211
 80212
 80213
 80214
 80215
 80216
 80217
 80218
 80219
 80220
 80221
 80222
 80223
 80224
 80225
 80226
 80227
 80228
 80229
 80230
 80231
 80232
 80233
 80234
 80235
 80236
 80237
 80238
 80239
 80240
 80241
 80242
 80243
 80244
 80245
 80246
 80247
 80248
 80249
 80250
 80251
 80252
 80253
 80254
 80255
 80256
 80257
 80258
 80259
 80260
 80261
 80262
 80263
 80264
 80265
 80266
 80267
 80268
 80269
 80270
 80271
 80272
 80273
 80274
 80275
 80276
 80277
 80278
 80279
 80280
 80281
 80282
 80283
 80284
 80285
 80286
 80287
 80288
 80289
 80290
 80291
 80292
 80293
 80294
 80295
 80296
 80297
 80298
 80299
 80300
 80301
 80302
 80303
 80304
 80305
 80306
 80307
 80308
 80309
 80310
 80311
 80312
 80313
 80314
 80315
 80316
 80317
 80318
 80319
 80320
 80321
 80322
 80323
 80324
 80325
 80326
 80327
 80328
 80329
 80330
 80331
 80332
 80333
 80334
 80335
 80336
 80337
 80338
 80339
 80340
 80341
 80342
 80343
 80344
 80345
 80346
 80347
 80348
 80349
 80350
 80351
 80352
 80353
 80354
 80355
 80356
 80357
 80358
 80359
 80360
 80361
 80362
 80363
 80364
 80365
 80366
 80367
 80368
 80369
 80370
 80371
 80372
 80373
 80374
 80375
 80376
 80377
 80378
 80379
 80380
 80381
 80382
 80383
 80384
 80385
 80386
 80387
 80388
 80389
 80390
 80391
 80392
 80393
 80394
 80395
 80396
 80397
 80398
 80399
 80400
 80401
 80402
 80403
 80404
 80405
 80406
 80407
 80408
 80409
 80410
 80411
 80412
 80413
 80414
 80415
 80416
 80417
 80418
 80419
 80420
 80421
 80422
 80423
 80424
 80425
 80426
 80427
 80428
 80429
 80430
 80431
 80432
 80433
 80434
 80435
 80436
 80437
 80438
 80439
 80440
 80441
 80442
 80443
 80444
 80445
 80446
 80447
 80448
 80449
 80450
 80451
 80452
 80453
 80454
 80455
 80456
 80457
 80458
 80459
 80460
 80461
 80462
 80463
 80464
 80465
 80466
 80467
 80468
 80469
 80470
 80471
 80472
 80473
 80474
 80475
 80476
 80477
 80478
 80479
 80480
 80481
 80482
 80483
 80484
 80485
 80486
 80487
 80488
 80489
 80490
 80491
 80492
 80493
 80494
 80495
 80496
 80497
 80498
 80499
 80500
 80501
 80502
 80503
 80504
 80505
 80506
 80507
 80508
 80509
 80510
 80511
 80512
 80513
 80514
 80515
 80516
 80517
 80518
 80519
 80520
 80521
 80522
 80523
 80524
 80525
 80526
 80527
 80528
 80529
 80530
 80531
 80532
 80533
 80534
 80535
 80536
 80537
 80538
 80539
 80540
 80541
 80542
 80543
 80544
 80545
 80546
 80547
 80548
 80549
 80550
 80551
 80552
 80553
 80554
 80555
 80556
 80557
 80558
 80559
 80560
 80561
 80562
 80563
 80564
 80565
 80566
 80567
 80568
 80569
 80570
 80571
 80572
 80573
 80574
 80575
 80576
 80577<br

1 confidential and securely maintained, to use this information for business purposes only, and to
 2 make only authorized disclosures of this information.

3 ***The Data Breach was a
 4 Foreseeable Risk of which Defendant was on Notice***

5 58. It is well known that PII, including Social Security numbers in particular, is a
 6 valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect
 7 such information, including Convergent, are well-aware of the risk of being targeted by
 8 cybercriminals.

9 59. Individuals place a high value not only on their PII, but also on the privacy of that
 10 data. Identity theft causes severe negative consequences to its victims, as well as severe distress
 11 and hours of lost time trying to fight against the impact of identity theft.

12 60. A data breach increases the risk of becoming a victim of identity theft. Victims of
 13 identity theft can suffer from both direct and indirect financial losses. According to a research
 14 study published by the Department of Justice, “[a] direct financial loss is the monetary amount
 15 the offender obtained from misusing the victim’s account or personal information, including the
 16 estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any
 17 losses that were reimbursed to the victim. An indirect loss includes any other monetary cost
 18 caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses
 19 that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included
 20 in the calculation of out-of-pocket loss.”²²

21 61. Individuals, like Plaintiff(s) and Class members, are particularly concerned with
 22 protecting the privacy of their Social Security numbers, which are the key to stealing any person’s
 23 identity and is likened to accessing your DNA for hacker’s purposes.

24 62. Data Breach victims suffer long-term consequences when their social security

²² “Victims of Identity Theft, 2018,” U.S. Department of Justice (April 2021, NCJ 256085) available at: <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last accessed November 1, 2022).

1 numbers are taken and used by hackers. Even if they know their social security numbers are being
 2 misused, Plaintiff(s) and Class Members cannot obtain new numbers unless they become a victim
 3 of social security number misuse.

4 63. The Social Security Administration has warned that “a new number probably
 5 won’t solve all your problems. This is because other governmental agencies (such as the IRS and
 6 state motor vehicle agencies) and private businesses (such as banks and credit reporting
 7 companies) will have records under your old number. Along with other personal information,
 8 credit reporting companies use the number to identify your credit record. So using a new number
 9 won’t guarantee you a fresh start. This is especially true if your other personal information, such
 as your name and address, remains the same.”²³

10 64. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020’s
 11 total of 1,108 and the previous record of 1,506 set in 2017.²⁴

12 65. Additionally in 2021, there was a 15.1% increase in cyberattacks and data
 13 breaches since 2020. Over the next two years, in a poll done on security executives, they have
 14 predicted an increase in attacks from “social engineering and ransomware” as nation-states and
 15 cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely
 come from “misconfigurations, human error, poor maintenance, and unknown assets.”²⁵

16 66. In light of high-profile data breaches at other industry leading companies,
 17 including Microsoft (250 million records, December 2019), Wattpad (268 million records, June
 18 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January
 19 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion
 20 records, May 2020), Convergent knew or should have known that its computer network would
 be targeted by cybercriminals.

21
 22 ²³ <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed November 1, 2022).

23 ²⁴ <https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/> (last accessed November 1, 2022).

24 ²⁵ <https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864> (last accessed November 1, 2022).

67. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

68. According to an FBI publication, “[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.”²⁶ This publication also explains that “[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn’t guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity.”²⁷

69. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Convergent failed to take appropriate steps to protect the PII of Plaintiff(s) and the proposed Class from being compromised.

70. Convergent failed to abide by its own Privacy Policy.²⁸

At All Relevant Times Convergent Had a Duty to Plaintiff(s) and Class Members to Properly Secure their Private Information

71. At all relevant times, Convergent had a duty to Plaintiff(s) and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff(s) and Class Members, and to promptly

²⁶ <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware> (last accessed November 1, 2022).

27 *Id.*

²⁸ <https://www.convergentusa.com/outsourcing/page/privacy-policy#q2> (last accessed on November 1, 2022).

1 notify Plaintiff(s) and Class Members when Convergent became aware that their PII was
 2 compromised.

3 72. Convergent had the resources necessary to prevent the Data Breach but neglected
 4 to adequately invest in security measures, despite its obligation to protect such information.
 5 Accordingly, Convergent breached its common law, statutory, and other duties owed to
 6 Plaintiff(s) and Class Members.

7 73. Security standards commonly accepted among businesses that store PII using the
 8 internet include, without limitation:

- 9 a. Maintaining a secure firewall configuration;
- 10 b. Maintaining appropriate design, systems, and controls to limit user access to
 certain information as necessary;
- 11 c. Monitoring for suspicious or irregular traffic to servers;
- 12 d. Monitoring for suspicious credentials used to access servers;
- 13 e. Monitoring for suspicious or irregular activity by known users;
- 14 f. Monitoring for suspicious or unknown users;
- 15 g. Monitoring for suspicious or irregular server requests;
- 16 h. Monitoring for server requests for PII;
- 17 i. Monitoring for server requests from VPNs; and
- 18 j. Monitoring for server requests from Tor exit nodes.

19 74. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud
 20 committed or attempted using the identifying information of another person without authority.”²⁹
 21 The FTC describes “identifying information” as “any name or number that may be used, alone
 22 or in conjunction with any other information, to identify a specific person,” including, among
 23 other things, “[n]ame, Social Security number, date of birth, official State or government issued
 24 driver’s license or identification number, alien registration number, government passport

²⁹ 17 C.F.R. § 248.201 (2013).

1 number, employer or taxpayer identification number.”³⁰

2 75. The ramifications of Convergent’s failure to keep consumers’ PII secure are long
 3 lasting and severe. Once PII is stolen, particularly Social Security and driver’s license numbers,
 4 fraudulent use of that information and damage to victims including Plaintiff(s) and the Class may
 5 continue for years.

6 ***The Value of Personal Identifiable Information***

7 76. The PII of consumers remains of high value to criminals, as evidenced by the
 8 prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen
 9 identity credentials. For example, personal information can be sold at a price ranging from \$40
 10 to \$200.³¹

11 77. Criminals can also purchase access to entire company’s data breaches from \$900
 12 to \$4,500.³²

13 78. Social Security numbers, for example, are among the worst kind of personal
 14 information to have stolen because they may be put to a variety of fraudulent uses and are difficult
 15 for an individual to change. The Social Security Administration stresses that the loss of an
 16 individual’s Social Security number, as is the case here, can lead to identity theft and extensive
 17 financial fraud:

18 A dishonest person who has your Social Security number can use it to get other
 19 personal information about you. Identity thieves can use your number and your
 20 good credit to apply for more credit in your name. Then, they use the credit cards
 21 and don’t pay the bills, it damages your credit. You may not find out that someone
 22 is using your number until you’re turned down for credit, or you begin to get calls
 23 from unknown creditors demanding payment for items you never bought.
 24 Someone illegally using your Social Security number and assuming your identity
 25 can cause a lot of problems.³³

20
 21 ³⁰ *Id.*

22 ³¹ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16,
 23 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed November 1, 2022).

24 ³² *In the Dark*, VPNOversight, 2019, available at: <https://vpnoversight.com/privacy/anonymous-browsing/in-the-dark/> (last accessed November 1, 2022).

³³ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed November 1, 2022).

1 79. Attempting to change or cancel a stolen Social Security number is difficult if not
 2 nearly impossible. An individual cannot obtain a new Social Security number without evidence
 3 of actual misuse. In other words, preventive action to defend against the possibility of misuse of
 4 a Social Security number is not permitted; an individual must show evidence of actual, ongoing
 5 fraud activity to obtain a new number.

6 80. Even a new Social Security number may not be effective, as “[t]he credit bureaus
 7 and banks are able to link the new number very quickly to the old number, so all of that old bad
 8 information is quickly inherited into the new Social Security number.”³⁴

9 81. This data, as one would expect, demands a much higher price on the black market.
 10 Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit
 11 card information, personally identifiable information and Social Security Numbers are worth
 12 more than 10x on the black market.”³⁵

13 82. PII can be used to distinguish, identify, or trace an individual’s identity, such as
 14 their name and Social Security number. This can be accomplished alone, or in combination with
 15 other personal or identifying information that is connected or linked to an individual, such as
 16 their birthdate, birthplace, and mother’s maiden name.³⁶

17 83. Given the nature of this Data Breach, it is foreseeable that the compromised PII
 18 can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the
 19 cybercriminals who possess Class Members’ PII can easily obtain Class Members’ tax returns or
 20 open fraudulent credit card accounts in Class Members’ names.

21 84. The Private Information compromised in this Data Breach is static and difficult,

22 ³⁴ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9,
 23 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last accessed November 1, 2022).

24 ³⁵ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed November 1, 2022).

25 ³⁶ See OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1 (last accessed November 1,
 26 2022).

1 if not impossible, to change (such as Social Security numbers).

2 85. Moreover, Convergent has offered only a limited subscription for identity theft
 3 monitoring and identity theft protection through IDX. Its limitation is inadequate when IDX's
 4 victims are likely to face many years of identity theft.

5 86. Furthermore, Defendant Convergent's credit monitoring offer and advice to
 6 Plaintiff(s) and Class Members squarely places the burden on Plaintiff(s)(s) and Class Members,
 7 rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In
 8 other words, Convergent expects Plaintiff(s) and Class Members to protect themselves from its
 9 tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff(s) and
 10 Class Members in credit monitoring services upon discovery of the breach, Defendant merely
 11 sent instructions to Plaintiff(s) and Class Members about actions they can affirmatively take to
 12 protect themselves.

13 87. These services are wholly inadequate as they fail to provide for the fact that
 14 victims of data breaches and other unauthorized disclosures commonly face multiple years of
 15 ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for
 16 the unauthorized release and disclosure of Plaintiff(s)' and Class Members' PII.

17 88. The injuries to Plaintiff(s) and Class Members were directly and proximately
 18 caused by Convergent's failure to implement or maintain adequate data security measures for the
 19 victims of its Data Breach.

Convergent Failed to Comply with FTC Guidelines

20 89. Federal and State governments have established security standards and issued
 21 recommendations to mitigate the risk of data breaches and the resulting harm to consumers and
 22 financial institutions. The FTC has issued numerous guides for business highlighting the
 23 importance of reasonable data security practices. According to the FTC, the need for data security
 24

1 should be factored into all business decision-making.³⁷

2 90. In 2016, the FTC updated its publication, *Protecting Personal Information: A*
 3 *Guide for Business*, which established guidelines for fundamental data security principles and
 4 practices for business.³⁸ The guidelines note businesses should protect the personal consumer
 5 and consumer information that they keep, as well as properly dispose of personal information
 6 that is no longer needed; encrypt information stored on computer networks; understand their
 7 network's vulnerabilities; and implement policies to correct security problems.

8 91. The FTC emphasizes that early notification to data breach victims reduces
 9 injuries: "If you quickly notify people that their personal information has been compromised,
 10 they can take steps to reduce the chance that their information will be misused" and "thieves who
 11 have stolen names and Social Security numbers can use that information not only to sign up for
 12 new accounts in the victim's name, but also to commit tax identity theft. People who are notified
 13 early can take steps to limit the damage."³⁹

14 92. The FTC recommends that companies verify that third-party service providers
 15 have implemented reasonable security measures.⁴⁰

16 93. The FTC recommends that businesses:

- 17 a. Identify all connections to the computers where you store sensitive
 18 information.
- 19 b. Assess the vulnerability of each connection to commonly known or
 20 reasonably foreseeable attacks.
- 21 c. Do not store sensitive consumer data on any computer with an internet

22 ³⁷ Federal Trade Commission, *Start With Security*, available at:
<https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed
 23 November 1, 2022).

24 ³⁸ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at:
<https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>
 (last accessed November 1, 2022).

³⁹ <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business> (last accessed
 November 1, 2022).

⁴⁰ FTC, *Start With Security*, *supra* note 37.

1 connection unless it is essential for conducting their business.

2

3 d. Scan computers on their network to identify and profile the operating system

4 and open network services. If services are not needed, they should be disabled

5 to prevent hacks or other potential security problems. For example, if email

6 service or an internet connection is not necessary on a certain computer, a

7 business should consider closing the ports to those services on that computer

8 to prevent unauthorized access to that machine.

9

10 e. Pay particular attention to the security of their web applications—the software

11 used to give information to visitors to their websites and to retrieve

12 information from them. Web applications may be particularly vulnerable to a

13 variety of hack attacks

14 f. Use a firewall to protect their computers from hacker attacks while it is

15 connected to a network, especially the internet.

16 g. Determine whether a border firewall should be installed where the business's

17 network connects to the internet. A border firewall separates the network

18 from the internet and may prevent an attacker from gaining access to a

19 computer on the network where sensitive information is stored. Set access

20 controls—settings that determine which devices and traffic get through the

21 firewall—to allow only trusted devices with a legitimate business need to

22 access the network. Since the protection a firewall provides is only as

23 effective as its access controls, they should be reviewed periodically.

24 h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an

eye out for activity from new users, multiple log-in attempts from unknown

users or computers, and higher-than-average traffic at unusual times of the

day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly

large amounts of data being transmitted from their system to an unknown user.

1 If large amounts of information are being transmitted from a business' 2
network, the transmission should be investigated to make sure it is authorized.

3 94. The FTC has brought enforcement actions against businesses for failing to protect 4
consumer and consumer data adequately and reasonably, treating the failure to employ 5
reasonable and appropriate measures to protect against unauthorized access to confidential 6
consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade 7
Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify 8
the measures businesses must take to meet their data security obligations.

9 95. Because Class Members entrusted Convergent with their PII, Convergent had, and 10
has, a duty to the Plaintiff(s) and Class Members to keep their PII secure.

10 96. Plaintiff(s) and the other Class Members reasonably expected that when they 11
provide PII to Convergent (or to Convergent's customers), Convergent would safeguard their 12
PII.

13 97. Convergent was at all times fully aware of its obligation to protect the personal 14
and financial data of consumers, including Plaintiff(s) and members of the Class. Convergent 15
was also aware of the significant repercussions if it failed to do so. Its own Privacy Policies, 16
quoted above, acknowledges this awareness.

17 98. Convergent's failure to employ reasonable and appropriate measures to protect 18
against unauthorized access to confidential consumer data—including Plaintiff(s)' and Class 19
Members' first names, last names, addresses, and Social Security numbers, and other highly 20
sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 21
5 of the FTCA, 15 U.S.C. § 45.

22 ***Plaintiff(s) and Class Members Have Suffered Concrete Injury as a Result of Defendant's***
Inadequate Security and the Data Breach it Allowed.

23 99. Plaintiff(s) and Class Members reasonably expected that Defendant would 24
provide adequate security protections for their PII, and Class Members provided Defendant with 25
sensitive personal information, including their names, addresses, and Social Security numbers.

1 100. Defendant's poor data security deprived Plaintiff(s) and Class Members of the
 2 benefit of their bargain. Plaintiff(s) and other individuals whose PII was entrusted with
 3 Convergent understood and expected that, as part of that business relationship, they would
 4 receive data security, when in fact Defendant did not provide the expected data security.
 5 Accordingly, Plaintiff(s) and Class Members received data security that was of a lesser value
 6 than what they reasonably expected. As such, Plaintiff(s) and the Class Members suffered
 7 pecuniary injury.

8 101. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Class
 9 Members are now, and for the rest of their lives will be, at a heightened and substantial risk of
 10 identity theft. Plaintiff(s) have also incurred (and will continue to incur) damages in the form of,
 11 *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft
 12 protection services.

13 102. The cybercriminals who obtained the Class Members' PII may exploit the
 14 information they obtained by selling the data in so-called "dark markets" or on the "dark web."
 15 Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals
 16 can pair the data with other available information to commit a broad range of fraud in a Class
 17 Member's name, including but not limited to:

- 18 • obtaining employment;
- 19 • obtaining a loan;
- 20 • applying for credit cards or spending money;
- 21 • filing false tax returns;
- 22 • stealing Social Security and other government benefits; and
- 23 • applying for a driver's license, birth certificate, or other public document.

24 103. In addition, if a Class Member's Social Security number is used to create false
 1 identification for someone who commits a crime, the Class Member may become entangled in
 2 the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

2 104. As a direct and/or proximate result of Defendant's wrongful actions and/or

1 inaction and the resulting Data Breach, Plaintiff(s) and the other Class Members have been
 2 deprived of the value of their PII, for which there is a well-established national and international
 3 market.

4 105. Furthermore, PII has a long shelf-life because it contains different forms of
 5 personal information, it can be used in more ways than one, and it typically takes time for an
 6 information breach to be detected.

7 106. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data
 8 Breach have also placed Plaintiff(s) and the other Class Members at an imminent, immediate,
 9 and continuing increased risk of identity theft and identity fraud. Indeed, “[t]he level of risk is
 10 growing for anyone whose information is stolen in a data breach.” Javelin Strategy & Research,
 11 a leading provider of quantitative and qualitative research, notes that “[t]he theft of SSNs places
 12 consumers at a substantial risk of fraud.”⁴¹ Moreover, there is a high likelihood that significant
 13 identity fraud and/or identity theft has not yet been discovered or reported. Even data that have
 14 not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now
 15 possess Class Members' PII will do so at a later date or re-sell it.

16 107. As a result of the Data Breach, Plaintiff(s) and Class Members have already
 17 suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

18 108. Although Convergent admits that the “the unauthorized actor deployed certain
 19 data extraction tools” on its computer systems. Cybercriminals actually exfiltrated the PII that
 20 was accessed.⁴²

19 *Plaintiff Guy's Experience*

20 109. Plaintiff Leo Guy is, and at all times relevant to this Complaint was, a resident
 21 and citizen of the State of New Hampshire.

22 ⁴¹ The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In
 23 Four Major Metropolitan Areas, (available at
https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last
 24 accessed November 1, 2022).

⁴² See Notice Letter, Ex. A.

1 110. Plaintiff Guy is a consumer who is apparently affiliated with a debt collection
2 customer of Convergent. Convergent required that either its customer or Plaintiff Guy to provide
3 it with his PII. Convergent was provided with his personal information, including but not limited
4 to his Social Security number.

5 111. On or about October 31, 2022, Plaintiff Guy received the Notice of Data Breach
6 letter, which indicated that Convergent had known about the Data Breach for over 4 months. The
7 letter informed him that his critical PII was accessed by an “unauthorized actor.” The letter stated
8 that the extracted information included his “name, contact information, financial account
9 number, and Social Security number” but did not expand on whether additional information was
stolen as well. See Guy Notice of Data Breach Letter, attached as Exhibit A.

10 112. Plaintiff Guy is alarmed by the amount of his Personal Information that was stolen
11 or accessed, and even more by the fact that his Social Security number was identified as among
12 the breach data on Convergent’s computer system.

13 113. For a couple of months now, Plaintiff Guy has been receiving a combination of
14 around 20 spam calls and many spam emails per day. Many of the spam emails include adult
15 related material or CBD products. His email spam has increased at least ten times since August
16 2022, to the point that he now receives up to fifty or so a day. Prior to this time, he was not
receiving the troublesome calls and emails.

17 114. Plaintiff Guy is concerned that the spam calls and texts are being placed with the
18 intent of obtaining more personal information from him and committing identity theft by way of
19 a social engineering attack.

20 115. In response to Convergent’s Notice of Data Breach, Plaintiff will be required to
21 spend time dealing with the consequences of the Data Breach, which will continue to include
22 time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring
23 and identity theft insurance options, and self-monitoring his accounts. They realize they will
24 likely have to spend about an hour a week verifying financial accounts to check for fraudulent
activities. The time they are forced to spend monitoring and securing their accounts has been lost

1 forever and cannot be recaptured.

2 116. Immediately after receiving the Notice Letter, Plaintiff spent time discussing his
 3 options with a law firm and has started to check his financial accounts in an effort to mitigate the
 4 damage that has been caused by Convergent.

5 117. Plaintiff is very careful about sharing PII and has never knowingly transmitted
 6 unencrypted PII over the internet or any other unsecured source.

7 118. Plaintiff suffered actual injury and damages as a result of the Data Breach.
 8 Plaintiff would not have provided Convergent with their PII had Convergent disclosed that it
 9 lacked data security practices adequate to safeguard PII.

10 119. Plaintiff suffered actual injury in the form of damages and diminution in the value
 11 of his PII—a form of intangible property that they entrusted to Convergent (or its customer).

12 120. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a
 13 result of the Data Breach and has anxiety and increased concerns for the loss of his privacy,
 14 especially his Social Security number.

15 121. Plaintiff Guy reasonably believes that his Private Information may have already
 16 been sold by the cybercriminals. Had he been notified of Convergent's breach in a timelier
 17 manner, he could have attempted to mitigate his injuries.

18 122. Plaintiff Guy has suffered imminent and impending injury arising from the
 19 substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII,
 20 especially his Social Security number, being placed in the hands of unauthorized third-parties
 21 and possibly criminals.

22 123. Plaintiff has a continuing interest in ensuring that his PII, which upon information
 23 and belief remains backed up and in Convergent's possession, is protected and safeguarded from
 24 future breaches.

CLASS ACTION ALLEGATIONS

23 124. Plaintiff(s) bring this action on behalf of themselves and on behalf of all other
 24 persons similarly situated ("the Class").

1 125. Plaintiff(s) propose the following Class definition, subject to amendment as
 2 appropriate:

3 All persons whose Private Information was maintained on Defendant Convergent
 4 Outsourcing, Inc.'s computer systems and compromised in Convergent's June 2022
 5 Data Breach.

6 126. Excluded from the Class are Defendant's officers and directors, and any entity in
 7 which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys,
 8 successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the
 9 judiciary to whom this case is assigned, their families and Members of their staff.

10 127. Plaintiff(s) hereby reserves the right to amend or modify the class definitions with
 11 greater specificity or division after having had an opportunity to conduct discovery.

12 128. Numerosity. The Members of the Class are so numerous that joinder of all of them
 13 is impracticable. While the exact number of Class Members is unknown to Plaintiff(s) at this
 14 time, based on information and belief, the Class consists of thousands of persons whose data was
 15 compromised in Data Breach.

16 129. Commonality. There are questions of law and fact common to the Class, which
 17 predominate over any questions affecting only individual Class Members. These common
 18 questions of law and fact include, without limitation:

- 19 A. Whether Defendant unlawfully used, maintained, lost, or disclosed
 20 Plaintiff(s)' and Class Members' Private Information;
- 21 B. Whether Defendant failed to implement and maintain reasonable security
 22 procedures and practices appropriate to the nature and scope of the
 23 information compromised in the Data Breach;
- 24 C. Whether Defendant's data security systems prior to and during the Data
 25 Breach complied with applicable data security laws and regulations;
- D. Whether Defendant's data security systems prior to and during the Data
 26 Breach were consistent with industry standards;
- E. Whether Defendant owed a duty to Class Members to safeguard their Private

Information;

- F. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- G. Whether computer hackers obtained Class Members' Private Information in the Data Breach;
- H. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- I. Whether Plaintiff(s) and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- J. Whether Defendant's conduct was negligent;
- K. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- L. Whether Defendant's acts, inactions, and practices complained of herein violated the Colorado data protection laws invoked below;
- M. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- N. Whether Plaintiff(s) and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

130. Typicality. Plaintiff(s)' claims are typical of those of other Class Members because Plaintiff(s)'s Private Information, like that of every other Class member, was compromised in the Data Breach.

131. Adequacy of Representation. Plaintiff(s) will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff(s)' Counsel are competent and experienced in litigating Class actions.

132. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff(s) and Class Members, in that all the Plaintiff(s)' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way.

1 The common issues arising from Defendant's conduct affecting Class Members set out above
 2 predominate over any individualized issues. Adjudication of these common issues in a single
 3 action has important and desirable advantages of judicial economy.

4 133. Superiority. A Class action is superior to other available methods for the fair and
 5 efficient adjudication of the controversy. Class treatment of common questions of law and fact
 6 is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most
 7 Class Members would likely find that the cost of litigating their individual claims is prohibitively
 8 high and would therefore have no effective remedy. The prosecution of separate actions by
 9 individual Class Members would create a risk of inconsistent or varying adjudications with
 10 respect to individual Class Members, which would establish incompatible standards of conduct
 11 for Defendant. In contrast, the conduct of this action as a Class action presents far fewer
 12 management difficulties, conserves judicial resources and the parties' resources, and protects the
 13 rights of each Class member.

14 134. Defendant has acted on grounds that apply generally to the Class as a whole, so
 15 that class certification, injunctive relief, and corresponding declaratory relief are appropriate on
 16 a Class-wide basis.

17 135. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for
 18 certification because such claims present only particular, common issues, the resolution of which
 19 would advance the disposition of this matter and the parties' interests therein. Such particular
 20 issues include, but are not limited to:

- 21 • Whether Defendant owed a legal duty to Plaintiff(s) and the Class to exercise due care in
 22 collecting, storing, and safeguarding their Private Information;
- 23 • Whether Defendant's security measures to protect its data systems were reasonable in
 24 light of best practices recommended by data security experts;
- 25 • Whether Defendant's failure to institute adequate protective security measures amounted
 26 to negligence;
- 27 • Whether Defendant failed to take commercially reasonable steps to safeguard consumer

1 Private Information; and

2 • Whether adherence to FTC data security recommendations, and measures recommended
3 by data security experts would have reasonably prevented the Data Breach.

4 136. Finally, all members of the proposed Class are readily ascertainable. Defendant
5 has access to Class Members' names and addresses affected by the Data Breach. Class Members
6 have already been preliminarily identified and sent notice of the Data Breach by Convergent.

7 **CAUSES OF ACTION**

8 **FIRST COUNT**

9 **Negligence**
10 **(On behalf of Plaintiff(s) and All Class Members)**

11 137. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully
12 set forth herein.

13 138. Convergent owed a duty to Plaintiff(s) and Class members to exercise reasonable
14 care in safeguarding and protecting their PII in its possession, custody, or control.

15 139. Plaintiff(s) and the Class Members entrusted their PII to Defendant with the
16 understanding that Defendant would safeguard their information.

17 140. Convergent had full knowledge of the sensitivity of the PII and the types of harm
18 that Plaintiff(s) and Class Members could and would suffer if the PII were wrongfully disclosed.

19 141. By assuming the responsibility to collect and store this data, and in fact doing so,
20 and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable
21 means to secure and safeguard its computer network—and Class Members' PII held within it—to
22 prevent disclosure of the information, and to safeguard the information from theft.
23 Defendant's duty included a responsibility to implement processes by which it could detect a
24 breach of its security systems in a reasonably expeditious period of time and to give prompt
notice to those affected in the case of a data breach.

25 142. Defendant had a duty to employ reasonable security measures under Section 5 of
the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or
affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of

1 failing to use reasonable measures to protect confidential data.

2 143. Defendant's duty to use reasonable care in protecting confidential data arose not
3 only as a result of the statutes and regulations described above, but also because Defendant is
4 bound by industry standards to protect confidential PII.

5 144. Defendant breached its duties, and thus was negligent, by failing to use reasonable
6 measures to protect Class Members' PII. The specific negligent acts and omissions committed
7 by Defendant include, but are not limited to, the following:

- 8 a. Failing to adopt, implement, and maintain adequate security measures to
safeguard Class Members' PII;
- 9 b. Failing to adequately monitor the security of its networks and systems;
- 10 c. Failing to periodically ensure that its email system had plans in place to
maintain reasonable data security safeguards;
- 11 d. Allowing unauthorized access to Class Members' PII; and
- 12 e. Failing to detect in a timely manner that Class Members' PII had been
compromised.

145. It was foreseeable that Defendant's failure to use reasonable measures to protect
15 Class Members' PII would result in injury to Class Members. Further, the breach of security was
16 reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the
17 industry.

146. It was therefore foreseeable that the failure to adequately safeguard Class
18 Members' PII would result in one or more types of injuries to Class Members.

147. There is a temporal and close causal connection between Defendant's failure to
19 implement security measures to protect the PII and the harm suffered, and an imminent and
20 substantial risk of harm that will be suffered by Plaintiff(s) and the Class.
21

22 148. As a result of Defendant's negligence, Plaintiff(s) and the Class Members have
23 suffered and will continue to suffer damages and injury including, but not limited to: out-of-
24 pocket expenses associated with procuring robust identity protection and restoration services;

1 increased risk of future identity theft and fraud, the costs associated therewith; time spent
 2 monitoring, addressing and correcting the current and future consequences of the Data Breach;
 3 and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

4 149. Plaintiff(s) and Class Members are entitled to compensatory and consequential
 damages suffered as a result of the Data Breach.

5 150. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring
 6 Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit
 7 to future annual audits of those systems and monitoring procedures; and (iii) continue to provide
 8 adequate credit monitoring to all Class Members.

9 **SECOND COUNT**

10 **Negligence *Per Se***

11 **(On Behalf of Plaintiff(s) and All Class Members)**

12 151. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully
 set forth herein.

13 152. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce,"
 14 including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such
 15 as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and
 16 orders described above also form part of the basis of Defendants' duty in this regard.

17 153. Convergent violated Section 5 of the FTC Act by failing to use reasonable
 18 measures to protect PII and not complying with applicable industry standards. Defendants'
 19 conduct was particularly unreasonable given the nature and amount of PII it obtained and stored,
 20 and the foreseeable consequences of the Data Breach for companies of Defendants' magnitude,
 21 including, specifically, the immense damages that would result to Plaintiff(s) and Members of
 22 the Class due to the valuable nature of the PII at issue in this case—including Social Security
 numbers.

23 154. Defendants' violations of Section 5 of the FTCA constitute negligence per se.

24 155. Plaintiff(s) and members of the Class are within the class of persons that the FTCA

1 was intended to protect.

2 156. The harm that occurred as a result of the Data Breach is the type of harm the
 3 FTCA was intended to guard against. The FTC has pursued enforcement actions against
 4 businesses, which, as a result of their failure to employ reasonable data security measures and
 5 avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff(s) and
 6 members of the Class.

7 157. As a direct and proximate result of Defendant's negligence per se, Plaintiff(s) and
 8 members of the Class have suffered and will suffer injury, including but not limited to: (i) actual
 9 identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise,
 10 publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention,
 11 detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v)
 12 lost opportunity costs associated with effort expended and the loss of productivity addressing and
 13 attempting to mitigate the actual and future consequences of the Data Breach, including but not
 14 limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud
 15 and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued
 16 risk to their PII, which remains in Defendants' possession and is subject to further unauthorized
 17 disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect
 18 the PII of customers in its continued possession; and (viii) future costs in terms of time, effort,
 19 and money that will be expended to prevent, detect, contest, and repair the impact of the PII
 20 compromised as a result of the Data Breach for the remainder of the lives of Plaintiff(s) and
 21 members of the Class.

22 158. Additionally, as a direct and proximate result of Defendants' negligence per se,
 23 Plaintiff(s) and members of the Class have suffered and will suffer the continued risks of
 24 exposure of their PII, which remains in Defendants' possession and is subject to further
 25 unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate
 26 measures to protect the PII in their continued possession.

27 159. Plaintiff(s)' and Class Members' Personal Information constitutes personal
 28

1 property that was stolen due to Convergent's negligence, resulting in harm, injury and damages
 2 to Plaintiff(s) and Class Members.

3 160. Convergent's conduct in violation of applicable laws directly and proximately
 4 caused the unauthorized access and disclosure of Plaintiff(s)' and Class Members' unencrypted
 5 Personal Information.

6 161. Plaintiff(s) and Class Members have suffered and will continue to suffer damages
 7 as a result of Convergent's conduct. Plaintiff(s) and Class Members seek damages and other
 8 relief as a result of Convergent's negligence.

9 **THIRD COUNT**

10 **Breach of Implied Contract**

11 **(On Behalf of Plaintiff(s) and All Class Members)**

12 162. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully
 13 set forth herein.

14 163. Plaintiff(s) and Class Members were required to provide their PII to Defendant as
 15 a condition of receiving other services provided by Defendant.

16 164. Plaintiff(s) and Class Members provided their PII to Defendant or its third-party
 17 agents in exchange for Convergent's services or employment. In exchange for the PII, Defendant
 18 promised to protect their PII from unauthorized disclosure.

19 165. At all relevant times Defendant promulgated, adopted, and implemented written
 20 a Privacy Policy whereby it expressly promised Plaintiff(s) and Class Members that it would only
 21 disclose PII under certain circumstances, none of which relate to the Data Breach.

22 166. On information and belief, Defendant further promised to comply with industry
 23 standards and to make sure that Plaintiff(s)' and Class Members' PII would remain protected.

24 167. Implicit in the agreement between Plaintiff(s) and Class Members and the
 25 Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes
 26 only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the
 27 PII, (d) provide Plaintiff(s) and Class Members with prompt and sufficient notice of any and all
 28

1 unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of
 2 Plaintiff(s) and Class Members from unauthorized disclosure or uses, (f) retain the PII only under
 3 conditions that kept such information secure and confidential.

4 168. When Plaintiff(s) and Class Members provided their PII to Defendant as a
 5 condition of relationship, they entered into implied contracts with Defendant pursuant to which
 6 Defendant agreed to reasonably protect such information.

7 169. Defendant required Class Members to provide their PII as part of Defendant's
 8 regular business practices.

9 170. In entering into such implied contracts, Plaintiff(s) and Class Members reasonably
 10 believed and expected that Defendant's data security practices complied with relevant laws and
 11 regulations and were consistent with industry standards.

12 171. Plaintiff(s) and Class Members would not have entrusted their PII to Defendant
 13 in the absence of the implied contract between them and Defendant to keep their information
 14 reasonably secure. Plaintiff(s) and Class Members would not have entrusted their PII to
 15 Defendant in the absence of its implied promise to monitor its computer systems and networks
 16 to ensure that it adopted reasonable data security measures.

17 172. Plaintiff(s) and Class Members fully and adequately performed their obligations
 18 under the implied contracts with Defendant.

19 173. Defendant breached its implied contracts with Class Members by failing to
 20 safeguard and protect their PII.

21 174. As a direct and proximate result of Defendant's breaches of the implied contracts,
 22 Class Members sustained damages as alleged herein.

23 175. Plaintiff(s) and Class Members are entitled to compensatory and consequential
 24 damages suffered as a result of the Data Breach.

25 176. Plaintiff(s) and Class Members are also entitled to nominal damages for the
 26 breach of implied contract.

27 177. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring

1 Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit
 2 to future annual audits of those systems and monitoring procedures; and (iii) immediately provide
 3 adequate long term credit monitoring to all Class Members for a period longer than the grossly
 4 inadequate one-year currently offered.

5 **FOURTH COUNT**

6 **Unjust Enrichment**

7 **(On Behalf of Plaintiff(s) and All Class Members)**

8 178. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully
 set forth herein.

9 179. Plaintiff(s) and Class Members conferred a monetary benefit on Defendant in the
 10 form of the provision of their PII and Defendant would be unable to engage in its regular course
 11 of business without that PII.

12 180. Defendant appreciated that a monetary benefit was being conferred upon it by
 Plaintiff(s) and Class Members and accepted that monetary benefit.

13 181. However, acceptance of the benefit under the facts and circumstances outlined
 14 above make it inequitable for Defendant to retain that benefit without payment of the value
 15 thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have
 16 expended on data security measures to secure Plaintiff(s)' and Class Members' Personal
 17 Information. Instead of providing a reasonable level of security that would have prevented the
 18 Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff(s)
 19 and Class Members by utilizing cheaper, ineffective security measures. Plaintiff(s) and Class
 20 Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to
 prioritize its own profits over the requisite data security.

21 182. Under the principles of equity and good conscience, Defendant should not be
 22 permitted to retain the monetary benefit belonging to Plaintiff(s) and Class Members, because
 23 Defendant failed to implement appropriate data management and security measures.

24 183. Defendant acquired the PII through inequitable means in that it failed to disclose

1 the inadequate security practices previously alleged.

2 184. If Plaintiff(s) and Class Members had known that Defendant had not secured their
3 PII, they would not have agreed to provide their PII to Defendant.

4 185. Plaintiff(s) and Class Members have no adequate remedy at law.

5 186. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class
6 Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft;
7 (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or
8 theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and
9 recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs
10 associated with effort expended and the loss of productivity addressing and attempting to mitigate
11 the actual and future consequences of the Data Breach, including but not limited to efforts spent
12 researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued
13 risk to their PII, which remain in Defendant's possession and is subject to further unauthorized
14 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
15 PII in their continued possession; and (vii) future costs in terms of time, effort, and money that
16 will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a
17 result of the Data Breach for the remainder of the lives of Plaintiff(s) and Class Members.

187. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class
19 Members have suffered and will continue to suffer other forms of injury and/or harm.

188. Defendant should be compelled to disgorge into a common fund or constructive
19 trust, for the benefit of Plaintiff(s) and Class Members, proceeds that they unjustly received from
20 them.

21 **FIFTH COUNT**

22 **Declaratory Judgment**

23 **(On Behalf of Plaintiff(s) and All Class Members)**

24 189. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully
set forth herein.

1 190. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is
 2 authorized to enter a judgment declaring the rights and legal relations of the parties and grant
 3 further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here,
 4 that are tortious and violate the terms of the federal and state statutes described in this Complaint.

5 191. An actual controversy has arisen in the wake of the Convergent data breach
 6 regarding its present and prospective common law and other duties to reasonably safeguard its
 7 customers' Personal Information and whether Convergent is currently maintaining data security
 8 measures adequate to protect Plaintiff(s) and Class members from further data breaches that
 compromise their Private Information.

9 192. Plaintiff(s) allege that Convergent's data security measures remain inadequate.
 10 Plaintiff(s) will continue to suffer injury because of the compromise of their Private Information
 11 and remain at imminent risk that further compromises of their Private Information will occur in
 12 the future.

13 193. Pursuant to its authority under the Declaratory Judgment Act, this Court should
 14 enter a judgment declaring, among other things, the following:

- 15 a. Convergent continues to owe a legal duty to secure consumers' Private
 16 Information and to timely notify consumers of a data breach under the common
 17 law, Section 5 of the FTC Act, and various states' statutes;
- 18 b. Convergent continues to breach this legal duty by failing to employ reasonable
 19 measures to secure consumers' Private Information.

20 194. The Court also should issue corresponding prospective injunctive relief requiring
 21 Convergent to employ adequate security protocols consistent with law and industry standards to
 22 protect consumers' Private Information.

23 195. If an injunction is not issued, Plaintiff(s) and Class members will suffer
 24 irreparable injury, and lack an adequate legal remedy, in the event of another data breach at
 Convergent. The risk of another such breach is real, immediate, and substantial. If another breach
 at Convergent occurs, Plaintiff(s) and class members will not have an adequate remedy at law
 because many of the resulting injuries are not readily quantified and they will be forced to bring
 multiple lawsuits to rectify the same conduct.

196. The hardship to Plaintiff(s) and class members if an injunction does not issue exceeds the hardship to Convergent if an injunction is issued. Among other things, if another massive data breach occurs at Convergent, Plaintiff(s) and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Convergent of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Convergent has a pre-existing legal obligation to employ such measures.

197. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Convergent, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff(s) pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff(s) and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff(s)' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiff(s) and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For declaratory relief as requested;

F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff(s) and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this Court may deem just and proper.

DATED this 2nd day of November 2022.

FRANK FREED SUBIT & THOMAS LLP

By: /s/ Michael C. Subit
Michael C. Subit, WSBA #29189
705 Second Avenue, Suite 1200
Seattle, WA 98104
Telephone: 206.624.6711
msubit@frankfreed.com

Local Counsel for Plaintiff(s)

MASON LLP

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
5101 Wisconsin Avenue, NW, Suite 305
Washington, DC 20016
Telephone: 202.429.2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Attorneys for Plaintiff(s)

**pro hac vice applications for admission to be filed.*